



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/648,770

08/27/2003

Ram Gopal Lakshmi Narayanan

27592-00454

4039

30678

7590

02/25/2008

CONNOLLY BOVE LODGE & HUTZ LLP
1875 EYE STREET, N.W.
SUITE 1100
WASHINGTON, DC 20036

EXAMINER

DINH, MINH

ART UNIT

PAPER NUMBER

2132

MAIL DATE

DELIVERY MODE

02/25/2008

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/648,770	Applicant(s) NARAYANAN, RAM GOPAL LAKSHMI	
	Examiner MINH DINH	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 08 November 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-16 and 33-46 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-16, 33-46 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 27 August 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

1. This action is in response to the RCE/amendment filed 11/08/07. Claims 1-4, 6-7, 11, 33 and 38 have been amended; claims 17-32 have been cancelled; claims 42-46 have been added.

Response to Arguments

2. Applicant's arguments, with respect to the rejections of claims 1-32 under 35 USC 112, first paragraph, as failing to comply with the enablement requirement, have been fully considered but they are not persuasive.

Applicant argues that the system "may or may not be a useful system, but it is a working system, and one of ordinary skill in the art would certainly be able to make and use it. This, alone, is sufficient for enablement." (page 10, second to last paragraph). Since a public key is different from its corresponding private key, one of ordinary skill in the art would not be able to make and use the claimed invention according to the disclosure.

Applicant states that, for the system to work when the public key and the private key are different, (i) the random value sent with the digital signature from the transmitting end may not be the same random value used to compute the digital signature at the receiving end; and (ii) the particular function used to generate the digital signature of the message at

Art Unit: 2132

the transmitting end may not be exactly the same as the one used to compute the digital signature at the receiving end (page 11, first paragraph). Applicant is required to submit detailed explanation to support those general statements in the next response because they are directed to a method/practice that is not well known for verifying a digital signature. Specifically, Applicant is required to show (i) how the receiver determines a random value to be used; (ii) how this random value is related to the random value used by the signer; (iii) what are the specific two different functions used by the signer (i.e., function 1 that takes as inputs the private key, random value 1, and the message) and the receiver (i.e., function 2 that is different from function 1 and takes as inputs the public key different from the private key, random value 2 different from random value 1, and the message); and (iv) proof showing that these two function generates the same digital signature. One of ordinary skills in the cryptography art would not be able to make and use the claimed invention without the information described above.

3. Applicant's arguments, with respect to the 35 USC 102(b) rejections have been fully considered but they are not persuasive. Applicant argues that the cited references fail to disclose or suggests a specific multicast channel to be used for other start-up messages to be used when the regular

Art Unit: 2132

start-up messages have not been received (page 13, first paragraph). Moy ("RFC 2328") discloses OSPF routing protocol which utilizes Hello protocol (page 31, Section 7.1 - The Hello Protocol). Moy specifically discloses that a router multicasts a Hello message when it starts (page 24, Section 4 – Functional Summary; page 43, Section 9.3 - The Interface State Machine: Down). The Hello message allows a neighboring router(s) to update its information regarding the status of the starting router (i.e., from previously Down) and to establish adjacency between the routers (page 50, Section 10.1 – Neighbor States). Therefore, the Hello message is functionally equivalent to a jump-start message. Moy further discloses that the starting router has not received any multicast protocol messages from other routers in the system since it was down (page 40, Section 9.1 – Interface States: Down).

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims 1-16, 42 and 45 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification

Art Unit: 2132

in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

Regarding claim 1, it recites the limitation "sending a jump-start message on said specific multicast channel from a start node ..., wherein the jump-start message is secured by the start node ...; receiving the jump-start message at a receiving node; and validating an authenticity of the jump-start message upon receipt of the start message at the receiving node." The specification discloses that the start node R1 generates a digital signature DS1 for the jump-start message by encrypting the source address and a random value using the private key of R1, i.e., $DS1 = \text{Enc}(\text{Source Address}, \text{Random Value}, \text{Private Key of Router 1})$ (paragraphs 0040-0045). The specification then discloses that the receiving node R2 receives the jump-start message together with signature DS1 and validates the authenticity of the jump-start message by: generating a digital signature DS2 by encrypting the source address and the random value retrieved from the start message using the public key of R1, i.e., $DS2 = \text{Enc}(\text{Source Address}, \text{Random Value}, \text{Public Key of Router 1})$; comparing DS1 and DS2, and determining that the start message is authentic if $DS1 = DS2$ (paragraphs 0046-0048). However, it is well known in cryptography art that the values of the public key and the private key of a public/private key pair are not supposed to be the same. As a result, the signatures DS1 and DS2 disclosed in the specification would

Art Unit: 2132

never be the same when the private key and the public key used in the process are valid keys and that the start message is authentic. Thus, the disclosure fails to enable one skilled in the art to make and use the claimed invention. Claims that are not specifically addressed are rejected by virtue of their dependency.

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 1-16, 42 and 45 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 1 recites the limitation "the nodes" and "said other nodes" in the providing step of claim 1. There is insufficient antecedent basis for this limitation in the claim. For examination purposes, the providing step is interpreted as "providing a specific multicast channel for sending a jump-start message by a node to other nodes when the node has not received any regular start-up messages from said other nodes on one or more multicast channels used for regular start-up messages".

Claim Rejections - 35 USC § 102

Art Unit: 2132

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claims 1-3, 5-6, 33-35, 37-40 and 42-46 are rejected under 35

U.S.C. 102(b) as being anticipated by Moy ("RFC 2328 – OSPF Version 2").

Moy discloses a method performed in a communication system including a plurality of nodes, i.e., routers implemented in OSPF routing protocol, communicating in a shared network segment and at least one multicast channel in said shared network segment (Section 1, Introduction; figure 1a, Broadcast networks), the method comprising: providing a specific multicast channel for multicasting a hello message by a node to other nodes when the node starts; sending a hello message together with a signature of the hello message on said specific multicast channel by a start node (i.e., the node that starts), wherein the signature is generated by the start node using a key, and wherein the start node starts an operation/an application and the start node has not received any multicast protocol messages from other node in the system since it was down (Section 4, Functional Summary; Section 7.1, The Hello Protocol; Section 9.1, Interface States; Section 9.3, The Interface State Machine; Section A.3.2, The Hello Packet; Section D.3, Cryptographic Authentication); receiving at a receiving node the hello message; and validating an authenticity of the hello message using the signature upon receipt of the hello message at the receiving node (Section D.5.3, Verifying Cryptographic Authentication; Security Consideration at the

Art Unit: 2132

end of the paper). The Hello message allows a neighboring router(s) to update its information regarding the status of the starting router (i.e., from previously Down) and to establish adjacency between the routers (page 50, Section 10.1, Neighbor States). Therefore, the Hello message is functionally equivalent to a jump-start message.

9. Claims 1-6, 33-35, 37-40 and 42-46 are rejected under 35 U.S.C. 102(b) as being anticipated by Murphy et al. ("Digital Signature Protection of the OSPF Routing Protocol") as evidenced by Moy ("RFC 2328 – OSPF Version 2"). Murphy discloses protection of routing information exchanged between routers in OSPF routing protocol using digital signature (Abstract). Specifically, Murphy discloses that when a sending router sends routing information message to a receiving router, the sending router signs the message using its private key so that the receiving router can verify the signature using the public key of the sending router to determine the authenticity of the message (Section 4, Using digital signature in OSPF). Murphy does not explicitly disclose multicasting a jump-start message including a hello message by a start node (i.e., a node that starts) that has not received any protocol messages since it was down; however, Moy discloses that this feature is inherent to the OSPF routing protocol (Section 1, Introduction; Section 4.3, Routing protocol packets; Section 7.1, The

Art Unit: 2132

Hello Protocol; Section 9.1, Interface States; Section 9.3, The Interface State Machine; Section A.3.2, The Hello Packet).

10. Claims 1-8, 10-12 and 33-46 are rejected under 35 U.S.C. 102(b) as being anticipated by Nguyen et al. (2002/0016926) as evidence by Moy ("RFC 2328 – OSPF Version 2").

Regarding claims 1-6, 33-35, 37-40 and 42-46 Nguyen discloses a method and system for securely exchanging routing information among routers, i.e., secure gateway devices (SGDs), in OSPF routing protocol using encryption (Abstract; paragraphs 0088, 0101). Specifically, Nguyen discloses that when a sending router sends routing information message to a receiving router, the sending router encrypts the message using an encryption key (paragraphs 0102, 0104-0105). Nguyen does not explicitly disclose multicasting a jump-start message including a hello message by a start node (i.e., a node that starts) that has not received any protocol messages since it was down; however, Moy discloses that this feature is inherent to the OSPF routing protocol (Section 1, Introduction; Section 4.3, Routing protocol packets; Section 7.1, The Hello Protocol; Section 9.1, Interface States; Section 9.3, The Interface State Machine; Section A.3.2, The Hello Packet).

Art Unit: 2132

Regarding claims 7-8, 10, 36 and 41, Nguyen does not explicitly disclose sending the multicast messages from the nodes comprising routers including a Designated Router and other routers; deciding that the Designated Router comprises an only available node in a shared segment if the Designated Router does not receive a response or the start message from the other nodes when only the Designated Router comprises an active node in a shared network segment; however, Moy discloses that this feature is inherent to the OSPF routing protocol (Section 1.2, Definitions of Commonly Used Terms; Section 4.3, Routing protocol packets; Section 7.1, The Hello Protocol; Section 7.3, The Designated Router). Nguyen further discloses generating a session key for encrypting multicast routing information, e.g., routing updates, using ISAKMP (paragraphs 104-105, 110-111).

Regarding claims 11-12 and 27-28, Nguyen further discloses engaging in Internet Key Exchange (IKE) protocol between routers involved in a communication session to generate security associations (paragraphs 0024-0025, 0105, 0119). Nguyen also discloses secure multicast communication among routers (paragraphs 0110-0111). Inherently, security associations used for unicast communication are different from those used for multicast communication.

Art Unit: 2132

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

12. Claims 13-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nguyen as evidence by Moy as applied to claim 1 above, and further in view of Srivastava et al. (7,103,185). Nguyen discloses using security associations for unicast/multicast communication between routers (paragraphs 0104-0105, 0110). Nguyen does not explicitly disclose a Designated Router and a Backup Designated Router connected (i.e., adjacent) to each other and to other routers in the network; however, Moy discloses that this feature is inherent to the OSPF routing protocol (Section 7.3, The Designated Router; Section 7.4, The Backup Designated Router). Nguyen does not disclose changing the session key for a multicast group when a new member joins the multicast group or when a member leaves the multicast group. Srivastava discloses a method for management of session keys in a multicast group comprising generating a new session key for a multicast group by a designated member when a new member joins the multicast group or when a member leaves the multicast group (col. 2, lines

Art Unit: 2132

58-67; figures 4B-C; col. 11, line 50 – col. 12, line 45). Srivastava also discloses generating a new session key for a multicast group when a member leaves the multicast group (col. 2, lines 58-67). It would have been obvious to one of ordinary in the art at the time the invention was made to modify the Nguyen method to change the session key for a multicast group when a new member joins the multicast group or when a member leaves the multicast group, as taught by Srivastava. The motivation for doing so would have been to prevent the new member from decrypting past messages and the member who leaves from deciphering future messages of the multicast group.

13. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nguyen as evidence by Moy as applied to claim 7, and further in view of Kaliski, Jr. (6,085,320). Nguyen, discloses using ISAKMP (Internet Security Association and Key Management Protocol) (paragraph 0105). Inherent to ISAKMP, each party in a two-party communication session generates a session key using a random number, its own private key and the other party's public key (according to Diffie-Hellman algorithm); however, a timestamp is not used to generate the session key in ISAKMP. Kaliski discloses using a timestamp (i.e., a time-varying value) in generating a session key (col. 5, lines 34-38). It would have been obvious to one of

Art Unit: 2132

ordinary in the art at the time the invention was made to modify the Nguyen method to use a timestamp in generating the session key, as taught by Kaliski, in order to prevent replay attack.

Allowable Subject Matter

14. Claim 16 is not rejected over prior art.

15. The following is a statement of reasons for the indication of allowable subject matter. Regarding claim 16, the limitations “generating using a Designated Router a new group key for all nodes when new Open Shortest Path First nodes join a network; first distributing the new group key to a Backup Designated Router using the Designated Router; next using the Designated Router and the Backup Designated Router to distribute the new key to all other nodes using respective unicast security association messages”, in combination with elements of the parent claims, have not been taught by prior art. The closest prior art, Harney et al. (“RFC 2094 – Group Key Management Protocol (GKMP) Architecture”), discloses that the designated group controller of a group either distributes a group key to each group member or broadcast the key to the group (Section 2.2.1); however, Harney does not disclose using help from a backup group controller in distributing the group key to each node.

Art Unit: 2132

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MINH DINH whose telephone number is (571)272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Art Unit: 2132

/M. D./
Examiner, Art Unit 2132

/Benjamin E Lanier/
Primary Examiner, Art Unit
2132

02/15/08